CHAPTER

15

TROUBLESHOOTING WINDOWS 2000

After reading this chapter and completing the exercises, you will be able to:

- Troubleshoot general problems with Windows 2000
- Understand some of the Windows 2000 troubleshooting tools
- Understand the Registry
- Work with advanced boot options

Windows 2000 troubleshooting is an important and vast arena. In this chapter, we discuss several aspects of detecting, isolating, and eliminating problems. The discussion includes material on installation failures, repair tools, printing solutions, and a collection of other pertinent and related issues.

General Principles of Troubleshooting

Troubleshooting is a tedious process of systematically eliminating problems in a computer system. You'll soon discover that troubleshooting is more often an art than an exact science. You should follow several common-sense guidelines to improve your troubleshooting skills and reduce system downtime.

Over the years, we've discovered that information is the most valuable asset you can possess when troubleshooting. Two types of information are key to troubleshooting: details about the computer and details about previous troubleshooting activities.

Computer Information File

A **Computer Information File (CIF)** is a detailed collection of all information related to the hardware and software products that make up your computer (and even your entire intranet). Actually, a CIF is not just a single file, but an ever-expanding accumulation of data sheets sorted into related groupings, which are in turn stored in a fireproof storage vault. Obviously, constructing a CIF from scratch is a lengthy process, but one that will be rewarded with averted problems, easy reconfigurations, and simplified replacement of failed components.

The organization of a CIF is not important; what is important is that the file contains thorough, specific, and accurate information about the products, configuration, setup, and problems associated with your intranet. Some method of correlating the data sheets to the actual components must be derived, such as an alpha-numeric labeling system.

Some of the important items you'll want to include in your CIF are as follows:

- The platform, type, brand, and model number of each component
- Complete manufacturer specifications
- Configuration settings, including jumpers and DIP switches, plus what each setting means, including IRQs, DMA addresses, memory base addresses, port assignments, and so forth
- The manual, user's guide, or configuration sheets
- The version of BIOS, driver software, patches, fixes, and so on, with floppy copies
- Printed and floppy copies of all parameter and initialization files
- A detailed directory structure printout
- The names and versions of all software
- Network-assigned names, locations, and addresses
- The status of empty ports, upgrade options, or expansion capabilities
- System requirements
- Warranty information
- Complete technical support contact information

- An error log with detailed and dated entries of problems and solutions
- The date and location of the last complete backup
- The location of backup items and original software
- A network layout and cabling map
- A date and initials on everything

Your CIF is not complete with just hardware and software details. You should also include the nonphysical characteristics of your system in the CIF, such as the following:

- Information services present
- Important productivity services
- Plans for future service deployment
- Hardware and software matched with services
- The structure of authorized access and security measures
- A training schedule
- A maintenance schedule
- A backup schedule
- Contact information for all system administrators
- Personnel organization or management hierarchy
- Workgroup arrangements
- Online data storage locations
- In-house content and delivery conventions
- Authorship rights and restrictions
- Troubleshooting procedures

Neither of these lists is exhaustive. As you operate and maintain your systems, you'll undoubtedly discover numerous other important data to add to this collection of information. Remember—if you don't document it, then you won't be able to find it when you really need it.

We recommend maintaining both a printed/written version of this material and an electronic version. Every time a change, update, or correction occurs, it should be documented in the electronic version, and a new printout should be made and stored. Murphy's law guarantees that the moment at which you will need your electronic data most is when your system will not function.

Common-Sense Troubleshooting

Unfortunately, the point at which you need to be most clear-headed and have plenty of time to solve problems is usually the exact moment when you are overworked, have lots of stress, or are under serious deadlines. Troubleshooting is a process that rarely offers satisfactory results when pursued with impatience and hostility. Here are some common-sense rules for getting the most out of your troubleshooting efforts:

- *Be patient*. Anger, frustration, hostility, and frantic impatience usually cause problems to intensify rather than dissipate.
- *Be familiar with your system's hardware and software.* If you don't know what baseline normal is, you may not know when a problem is solved or when new problems surface.
- *Attempt to isolate the problem.* When possible, eliminate segments or components that are functioning properly, thereby narrowing the range of suspects.
- *Repeal the most recent change.* The simplest fix is to undo the problem you just caused; attempt to expunge the most recent alteration, upgrade, or change made to your system.
- *Investigate the most common points of failure.* The most active or sensitive components are the most common points of failure; they include hard drives, cables, and connectors.
- *Recheck items that have caused problems in the past.* As the axiom goes, history does repeat itself (and usually right in your own backyard).
- *Do the easy and quick first.* Why punish yourself early? Try the easy fixes before moving on to the more time-consuming, difficult, or even destructive measures.
- *Let the fault guide you.* The old adage, "Where there is smoke, there is fire," applies to computer problems just as much as real life. Investigate related components and system areas associated with the suspected fault.
- *Make changes one at a time.* A step-by-step process enables you to clearly distinguish the solution when you stumble upon it.
- *Repeat the failure if possible.* In many cases, being able to repeat an error is the only way to locate it. Transient and inconsistent faults are difficult to uncover because of their "now you see it, now you don't" nature.
- *Keep a detailed solution and attempted solution log.* Keep track of everything you do (both successful and failed attempts). This log will prove an invaluable resource when an error occurs again on the same or a different system, or when the same system experiences a related problem.
- *Learn from others' mistakes*. Others' failures, if you study them, can save you from making the same mistake.

- *Learn from your own mistakes.* A wise administrator is the one who can look at his or her failures, and better himself or herself through them.

This list of common-sense items shouldn't contain much that you didn't already know. The most difficult part is remembering these guidelines when you are in the heat of battle.

TROUBLESHOOTING INSTALLATION PROBLEMS

Unfortunately, the installation process of Windows 2000 is susceptible to several errors: media errors, domain controller communication difficulties, stop message errors or halt on blue screen, hardware problems, and dependency failures. The following list contains a short synopsis of each error type.

- *Media errors:* Media errors are problems with the distribution CD-ROM itself, the copy of the distribution files on a network drive, or the communication link between the installation and the distribution files. The only regularly successful solution to media errors is to switch media—for example, copying the files to a network drive, linking to a server's CD-ROM, or installing a CD-ROM on the workstation. If you encounter media errors, always restart the installation process from the beginning.
- *Domain controller communication difficulties:* Communication with the domain controller is crucial to some installations, especially when attempting to join a domain. Most often this problem is related to a typing error (such as a name, password, or domain name), but network failures and offline domain controllers can be causes as well. Verify the viability of the domain controller directly and from other workstations (if applicable).
- *Stop message errors or halt on blue screen:* Use of an incompatible or damaged driver controller is the most common cause of stop messages and halting on the blue screen during installation. If any information is presented to you about an error, try to determine whether you are using the proper driver. Otherwise, double-check your hardware and the drivers that are required to operate them under Windows 2000.
- *Hardware problems:* If you failed to verify your hardware with the Hardware Compatibility List (HCL) or a physical defect has surfaced in previously operational devices, very strange errors can arise. In such cases, replacing the device is the only viable solution. Before you go to that expense, double-check the installation and configuration of all devices within the computer.
- *Dependency failures:* The failure of a service or driver due to the failure of a foundational or prior service or driver is known as a dependency failure. For example, the server and workstation services may fail because the NIC does not initialize properly. Often Windows 2000 will boot in spite of these errors, so check the Event log for more details.

Just knowing about these installation problems can help you avoid them. Unfortunately, successfully installing Windows 2000 does not eliminate the possibility of further complications. Luckily, Microsoft has included several troubleshooting tools that can help locate and eliminate most system failures, are discussed in the next section.

TROUBLESHOOTING TOOLS

The repair and troubleshooting tools native to Windows 2000 are components with which you need to become familiar. They are applicable to most situations and can save you countless hours of troubleshooting digression. The next few sections detail how to use the Event Viewer and the Computer Management tools.

Event Viewer

The **Event Viewer** is used to view system messages regarding the failure or success of various key occurrences within the Windows 2000 environment (see Figure 15-1). The items recorded in the Event Viewer's logs inform you of system drivers or service failures as well as security problems or aberrant applications. Located in the Administrative Tools section of the Control Panel and Start menu, this tool is used to view the logs created automatically by Windows 2000. These logs are as follows:

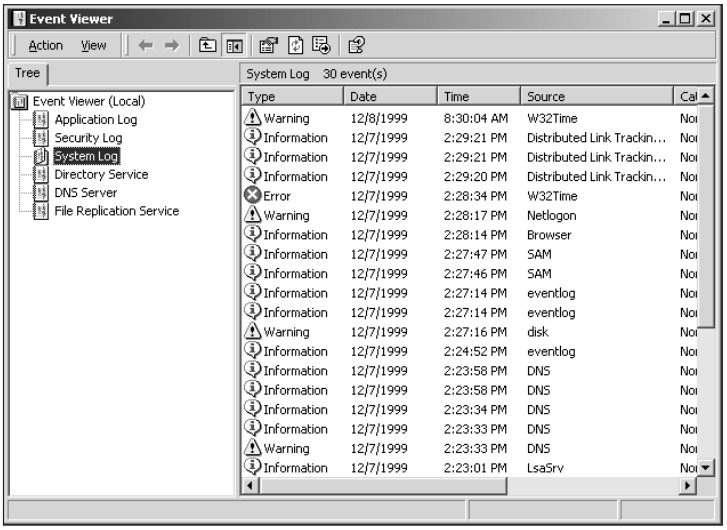

Figure 15-1 Event Viewer with System Log selected

- **Application Log**—Records application events, alerts, and system messages.
- **Directory Service Log**—Records events related to the Directory Service.
- **DNS Service Log**—Records events related to the DNS Service.

- **File Replication Service Log**—Records events related to the File Replication Service.
- **Security Log**—Records security-related events, including audit events.
- **System Log**—Records information and alerts about the Windows 2000 internal processes, including hardware and operating system errors, warnings, and general information messages.

Each log records a different type of event. All of the logs, however, collect the same meta-information about each event: date, time, source, category, event, user ID, and computer. Each logged event (see Figure 15-2) includes some level of detail about the error, ranging from an error code number to a detailed description with a memory HEX buffer capture. Most system errors, including stop errors that result in the blue screen, are recorded in the System log. You can therefore review the time and circumstances around a system failure. In many cases, the details in the Event Viewer can be used as pieces of evidence in your search for the actual cause of a problem. The event details offer little actual resolution information, however.

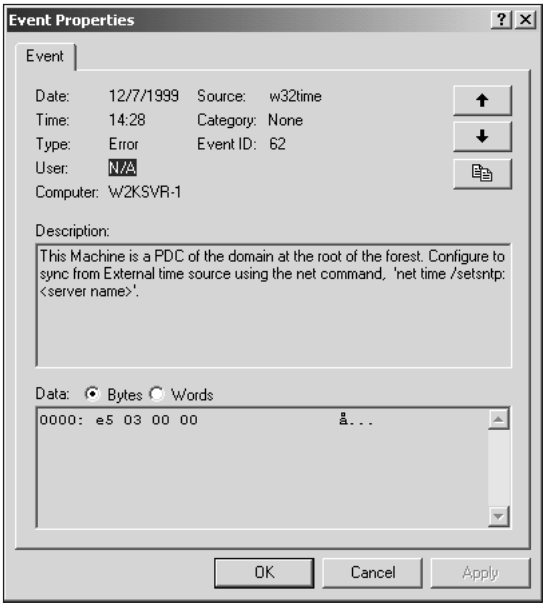

Figure 15-2 Event Viewer event detail

Computer Management

One of the most helpful advancements in the area of hardware support under Windows 2000 is the addition of Plug and Play capabilities to the robustness of Windows NT. A useful side effect of Plug and Play is greater simplicity of the troubleshooting tools, which can be brought to bear against nearly every aspect of Windows 2000. The bulk of these tools are collected into a single interface under the Computer Management tool found in the Administrative Tools section of the Control Panel and Start menu.

The Computer Management tool combines many tools from Windows NT, Windows 98, and several completely new utilities. This single interface (see Figure 15-3) makes locating and resolving problems on your key systems easier than ever before. The Computer Management collection of utilities is divided into three sections: System Tools, Storage, and Services and Applications. The Services and Applications section contains management controls for various installed and active services and applications. The actual contents of this section will depend on the state of your system. Some of the common controls are as follows:

- *Telephony*: For modem and remote communications
- *WMI Control*: For management of the Windows Management Instrumentation (WMI) service
- *Services:* For stopping and starting services as well as configuring the start-up parameters for services
- *Indexing Service:* For defining the corpus for Index Server
- *Internet Information Services:* For managing Internet services
- *DNS:* For managing the Domain Name Service

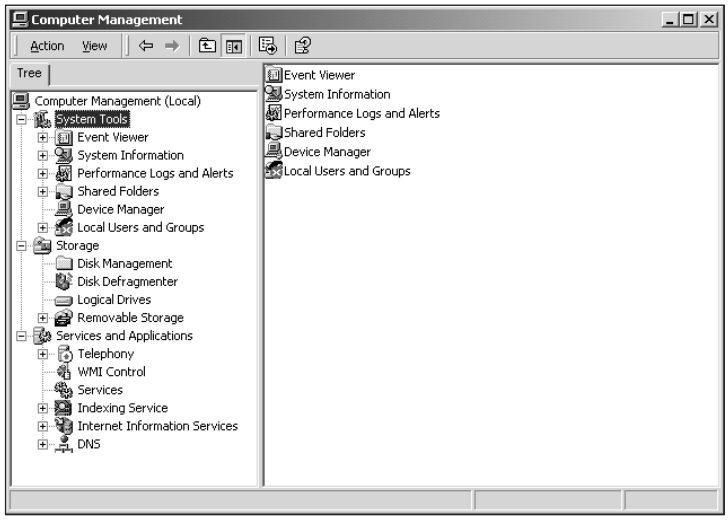

Figure 15-3 Computer Management

The System Tools section contains six tools. The Event Viewer is accessible here (as discussed earlier in this chapter). The System Information tool is used to access configuration information and status summaries for the computer and operating system environment. You can quickly discover information such as system model numbers, free IRQs, sharing conflicts, and component configurations. This tool is invaluable when attempting to add new hardware into your system. The third tool, the Performance Logs and Alerts tool, offers another means to access the Performance Monitoring tool of Windows 2000 (see Chapter 13 for details). Shared Folders is used to discover the shared folders existing on the local system. This

interface shows hidden shares, current sessions, and open files. The Device Manager enables you to view and alter the current hardware configurations of all existing devices. The Local Users and Groups tool is disabled when Active Directory is present; otherwise, it is used to create and manage local user accounts and groups.

The Storage section of Computer Management includes four tools that simplify storage device administration. The Disk Management tool allows you to view and alter the partitioning and volume configuration of hard drives. The Disk Defragmenter improves the layout of stored data on drives by reassembling fragmented files and aggregating free space. Logical Drives is used to gain information about logical drives (that is, those that you've formatted and assigned drive letters to). Removable Storage enables you to manage removable media, from floppies to tapes to whatever.

THE REGISTRY

Windows 2000 uses a system component called the **Registry** which is a database that stores data about a system's configuration in a hierarchical form. The Registry holds information essential to Windows 2000 itself as well as native applications, added services, and most add-on software products from Microsoft and third-party vendors. The information stored in the Registry is comparable to information stored in initialization (.ini, .dat, .bat, .sys, and so on) files in Windows 3.x or even Windows 95/98. For native Windows 2000 applications, the Registry takes the place of .ini files, storing all of their configuration information in this database. Although the Control Panel applets and the Administration Tools utilities suffice to cover most Windows 2000 configuration needs, some settings can be established or changed only by editing the Registry directly.

One important fact to keep in mind about the Registry is that it is not an exhaustive collection of configuration settings. Instead, it holds only the exceptions to the defaults. Processes within Windows 2000 will operate with their own known internal defaults unless a **value** in the Registry specifically alters that default behavior. This fact makes working with the Registry difficult, as most often the control you need is not contained in the Registry because the internal defaults are being used. To alter such a setting, you must know the exact syntax, spelling, location, and valid values; otherwise, you will be unable to modify the default behavior. For Windows NT 4.0, the Resource Kit contains a help file named Regentry.hlp that lists all of the possible Registry entries and valid values.

Each Registry **key** is similar to a bracketed heading in an .ini file. Changes made to system configurations through Administrative Tools or Control Panel applets are applied to the Registry database. A special kind of administrative tool, the Registry Editor, allows you to make changes directly to the Registry database. Such tools understand the hierarchical nature of the Registry and are capable of manipulating each level in the hierarchy.

The structure and layout of the Registry are not exactly human-friendly. Instead, this database was designed for programming ease and speed of interaction for processes. Its structure, although a bit daunting, is understandable if broken down into its parts. The Registry is divided into five major groupings, called keys. Below each key are one or more levels of **subkeys**. A

subkey is just another sublevel of grouping. Within each subkey, one or more values can exist. A **value entry** is a named parameter or placeholder for a control setting or configuration data. It can hold a single binary digit, a long string of ASCII characters, or a hexidecimal value. The actual data held by a value entry is known as the value. Figure 15-4 depicts the Registry's structure.

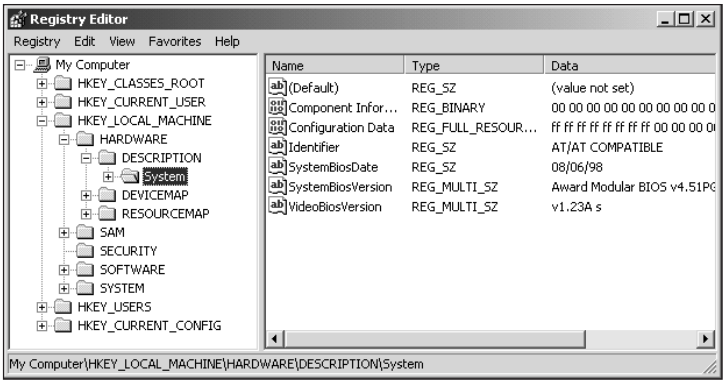

Figure 15-4 View of Registry hierarchy structure via the Registry Editor

Important points to keep in mind about the Registry include the following:

- Keys are the top-level or root divisions of the Registry.
- Keys can contain one or more subkeys.
- A subkey can contain one or more subkeys.
- A subkey can contain one or more value entries.

Each time Windows 2000 starts, the Registry is loaded into memory from files stored on the hard drive. Each time Windows 2000 shuts down, the Registry is written from memory back to the files. While Windows 2000 is operating, the Registry remains in memory. The Registry is therefore easy to access and quick to respond to control queries. Because it remains in memory, changes to the Registry take effect immediately. In most cases, any change made to the Registry immediately results in the use of that change as an operational parameter. Only in rare cases will Windows 2000 require a reboot to enforce changes.

As noted earlier, there are five top-level keys in the Registry. Each key has a unique purpose, as described in the following list:

- **HKEY_LOCAL_MACHINE**—This Registry key contains the value entries that control the local computer, including hardware devices, device drivers, and various operating system components. The data stored in this key is not dependent on a logged-on user or the applications or processes in use. (See Figure 15-5.)

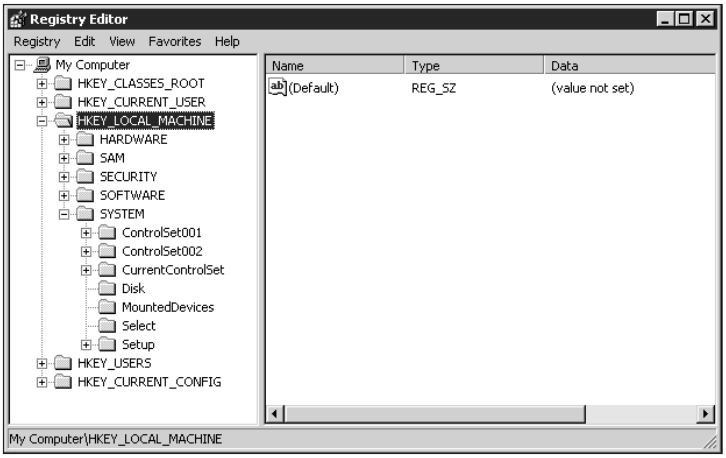

Figure 15-5 HKEY_LOCAL_MACHINE as viewed through the Registry Editor

- **HKEY_CLASSES_ROOT**—This Registry key contains the value entries that control the relationships between file extensions (and therefore file format types) and applications. It also supports the data used in object linking and embedding (OLE), COM object data, and file-class association data. This key actually points to another Registry key named HKEY_LOCAL_MACHINE\Software\Classes, and it provides multiple points of access to make itself easily accessible both to the operating system and to applications that need access to the compatibility information already mentioned. (See Figure 15-6.)

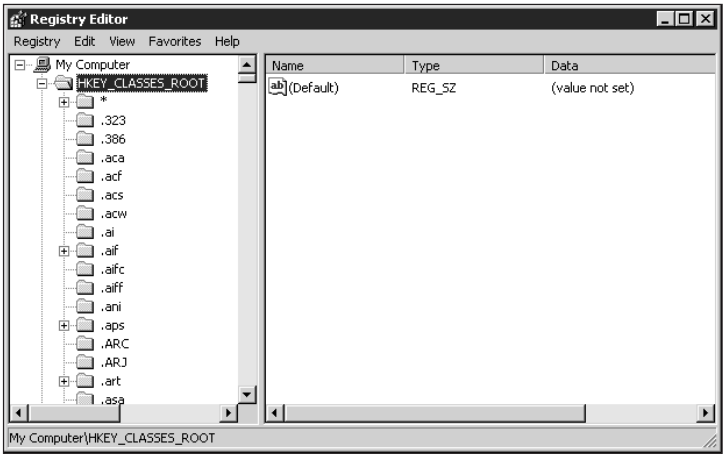

Figure 15-6 HKEY_CLASSES_ROOT as viewed through the Registry Editor

- **HKEY_CURRENT_CONFIG**—This Registry key contains the value entries that control the currently active hardware profile. Its contents are built each time the system starts up. This key is derived from data stored in the

HKEY_LOCAL_MACHINE\System\CurrentControlSet\HardwareProfiles subkey. It provides backward compatibility with Windows 95/98 applications. (See Figure 15-7.)

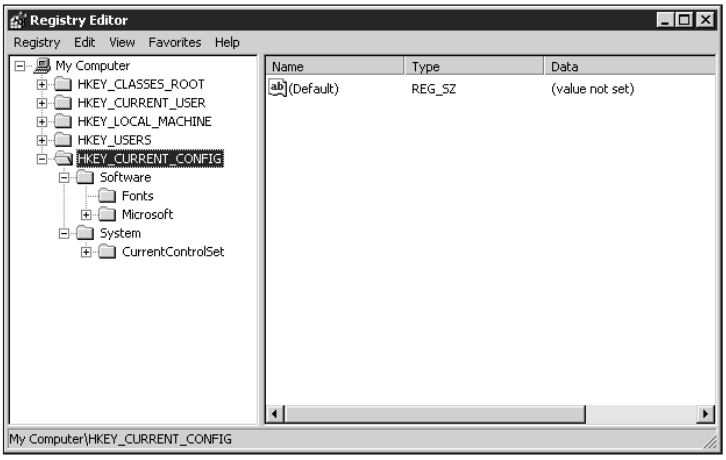

Figure 15-7 HKEY_CURRENT_CONFIG as viewed through the Registry Editor

- **HKEY_CURRENT_USER**—This Registry key contains the value entries that define the user environment for the currently logged-on user. It is built each time a user logs onto the system. The data in this key is derived from the HKEY_USERS key and the Ntuser.dat/.man file of a user's profile. (See Figure 15-8.)

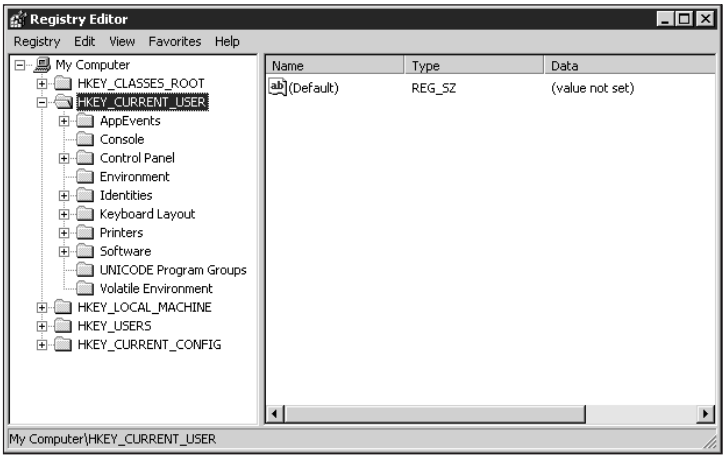

Figure 15-8 HKEY_CURRENT_USER as viewed through the Registry Editor

- **HKEY_USERS**—This Registry key contains the value entries that define the user environments for all users who have ever logged onto this computer. When a new user logs onto this system, a new subkey is added for that user which is

either built from the default profile stored in this key or constructed from the roaming user profile associated with the domain user account. (See Figure 15-9.)

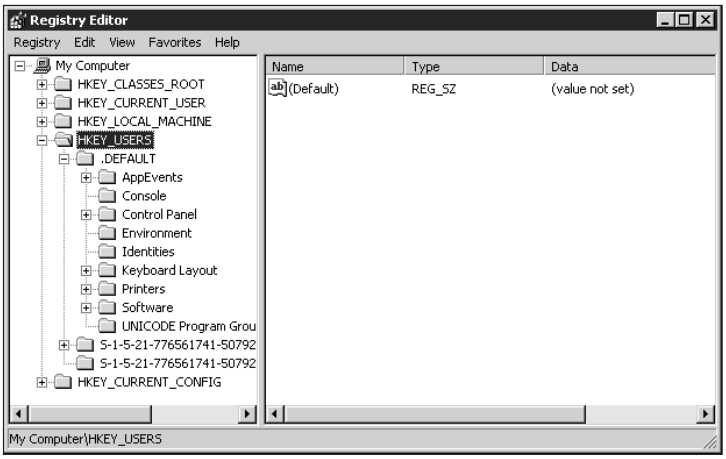

Figure 15-9 HKEY_USERS as viewed through the Registry Editor

In some instances, a sixth key may appear on Windows 2000. The HKEY_DYN_DATA key is used by some Windows 95 applications. When these applications are installed on a Windows 2000 system, the Windows 2000 Registry creates a pseudo-key that redirects calls to this sixth key to the alternative areas of the Registry, such as HKEY_CLASSES_ROOT, where the data actually reside.

About Value Entries

Value entries within the Registry consist of three parts: name, data type, and value. A Registry value entry's name is typically a multiword phrase without spaces that uses title capitalization—for example; AutoAdminLogon (see Figure 15-10).

The data type of a value entry tells the Registry how to store the value. This information is extremely important because an ACSII text string is different from a hex value, which is in turn different from binary data. The data type specifies whether the data consist of a text string or a number and the numerical base or radix of that number. Radix types supported by Windows 2000 are decimal (base 10), hexadecimal (base 16), and binary (base 2). All hexadecimal values are listed with the prefix "0x" to identify them clearly (as in 0xF for 15).

The value of a value entry is the actual data contained by that value entry. It can be of any length, and its content is limited only by its data type. Windows 2000 supports five data types:

- **REG_BINARY**—Binary format
- **REG_DWORD**—Binary, hex, or decimal format
- **REG_EXPAND_SZ**—Expandable text-string format that contains a variable that is replaced by an application when it is used (for example, %Systemroot%\file.exe)

- **REG_MULTI_SZ**—Text-string format that contains multiple human-readable values separated by NULL characters
- **REG_SZ**—Text-string format

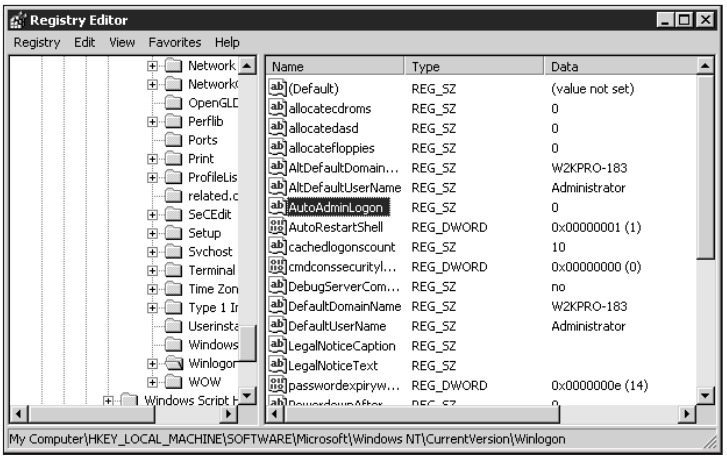

Figure 15-10 AutoAdminLogon as viewed through the Registry Editor

Once a value entry is created and its data type defined, that data type cannot be changed. To alter the data type of a value, you must delete the value entry and then re-create it with a new data type.

Registry Storage Files

The files used to store the Registry are located in the %systemroot%\system32\config directory of the boot partition (see Figure 15-11). The Registry is not stored in files that match one-to-one with the top-level keys. Instead, it is stored in various subkey, logging, and backup files, as shown in Table 15-1.

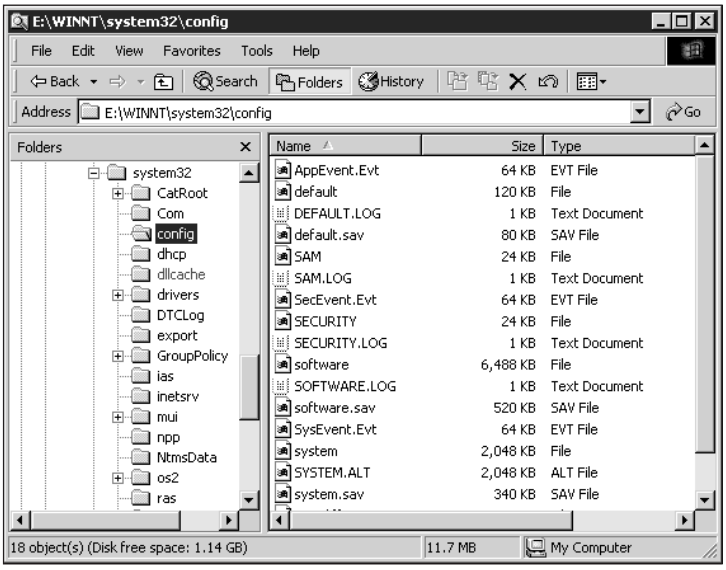

Figure 15-11 The contents of the %systemroot%\system32\config directory

Table 15-1 The storage files of the Registry

Registry hive	Filenames
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav
(Not associated with a hive)	Userdiff, Userdiff.log
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log

Notice that only four of the HKEY_LOCAL_MACHINE subkeys, the .DEFAULT subkey of the HKEY_USERS key, and the HKEY_CURRENT_USER key are stored in files. All of the other keys and subkeys are either built during the boot process or are copies of a subsection of HKEY_LOCAL_MACHINE.

The HKEY_USERS key is built from the default file (which represents the default user profile's Ntuser.dat file) and copies the profiles for all users who have ever logged onto the computer. These profiles are cached locally in \Documents and Settings\<username> directories. A copy of the Ntuser.dat or Ntuser.man file is copied into the repair directory for the currently logged-on user.

Notice that the Registry storage files use four extensions. The extension identifies the purpose or function of the particular file:

- *No extension:* The storage file for the subkey.
- *.alt:* The backup file of the subkey. Note that only the HKEY_LOCAL_MACHINE\System subkey has a backup file.
- *.log:* A file containing all changes made to a key. This file is used to verify that all modifications to the Registry are applied properly.
- *.sav:* Copies of a key in their original state as created at the end of the text portion of Windows 2000 installation.

The Registry Editors: REGEDIT and REGEDT32

Because the structure of the Registry is so complex, special tools are required to operate on it directly. In Windows 2000, you have two different Registry Editors from which to choose: **REGEDIT** and **REGEDT32**. The former is a 16-bit application, whereas the latter is a 32-bit application. REGEDIT (see Figure 15-12) offers global searching and combines all of the keys into a single display. REGEDT32 (see Figure 15-13) allows you greater control over key and value entry security, and displays each root key in a separate window. REGEDT32 also offers a read-only mode so you can explore without the possibility of accidentally altering value entries. Both editors can be used to perform searches, add new subkeys and value entries, alter the data in value entries, and import and export keys and subkeys. You'll need to get to know both editors to manipulate the Registry with great dexterity.

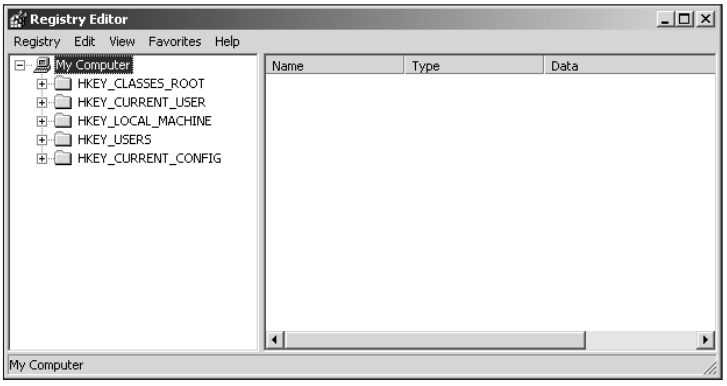

Figure 15-12 REGEDIT

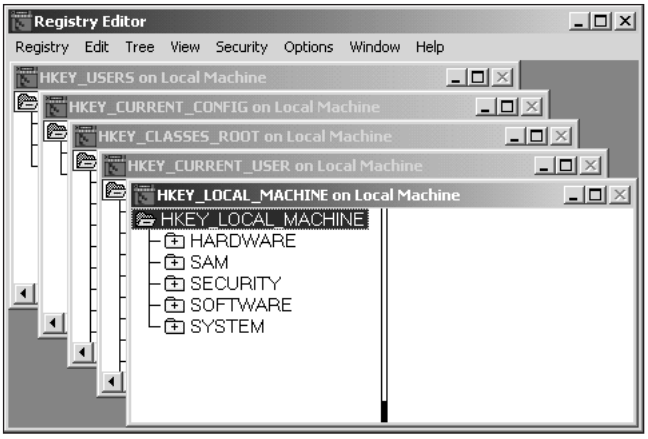

Figure 15-13 REGEDT32

Editing the Registry directly is a task that should not be undertaken without forethought and planning. It is easily possible to alter the Registry—whether on purpose or accidentally—in such a way as to render a system completely unrecoverable. If you don't know exactly what you are doing in the Registry, don't edit it! Even when you do think you know exactly what you wish to change in the Registry, it is always a good idea to take precautions.

- Back up all important data on the computer.
- Make a separate backup of all or part of the Registry. Saving each key or subkey individually is recommended. Store the backup files on local drives, network drives, and floppies or other removable media to ensure access.
- Restart the computer before editing the Registry.
- Perform only one Registry modification at a time. Test the results before proceeding.
- Reboot immediately after each change to force full system compliance. This step is not strictly necessary but has often proven a prudent measure.
- Always test the changes on a nonproduction system hosting noncritical services before deploying them on production systems.
- Use the REGEDT32 read-only mode to explore the Registry to ensure that accidental changes are not made.

Registry Size Limitations

As noted earlier, the Registry is stored in active memory, so it is quickly and easily accessible while the operating system is functioning. It resides in the paged pool portion of memory, which means it can be swapped out to disk when it is not in use. In contrast, the kernel resides in a nonpaged pool portion of memory, so it always stays in physical RAM. As your system ages, many changes will accumulate in the Registry, causing its size to grow. Its initial size on a Windows 2000 Professional system is approximately 10 MB. To prevent the

Registry from consuming too much memory, Windows 2000 imposes a maximum size for the Registry. This size ceiling is set at one-fourth of the current paged pool by default, although you can change it. When the page pool size changes, Windows 2000 will automatically adjust the Registry size ceiling as well.

To alter the Registry ceiling, open the Virtual Memory dialog box (the Change button appears on the Performance Options dialog box, which is accessed by clicking the Performance Options button on the Advanced tab of the System applet from the Control Panel). Then change the value in the number field beside Maximum registry size (MB) within the Registry size area (see Figure 15-14). This value sets the maximum boundary size only for the Registry; it does not allocate paged pool space or guarantee that paged pool space will even be available.

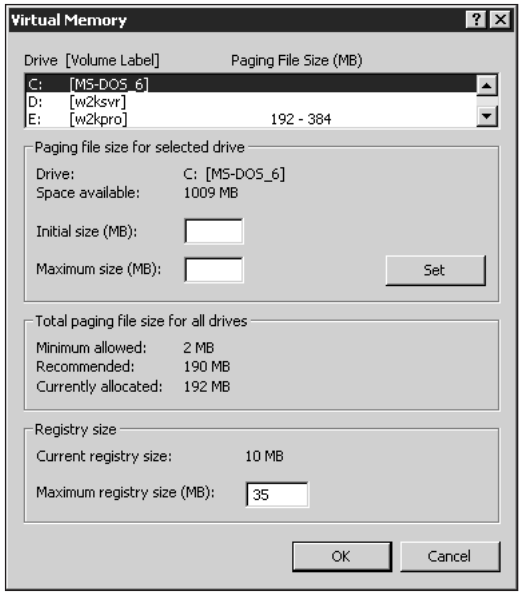

Figure 15-14 Virtual Memory dialog box, where the Registry size is defined

Backing Up the Registry

Even though Windows 2000 automatically manages the safety of the Registry via its fault-tolerance mechanisms (namely, .log and .alt files), it is still important for you to take proactive measures to back up the Registry. You can employ several methods to create reliable Registry backups:

- Most Windows 2000 backup applications include support for full Registry backups. With these products, you can back up the Registry as part of your daily automated backup or as a distinct Registry-only procedure.
- Either REGEDIT or REGEDT32 can be used to save all or part of the Registry to separate files.

- You can make a copy of the %systemroot%\System32\config directory manually.
- You can employ the *Windows 2000 Resource Kit* tools, Reg.exe or Regback.exe.

No matter which method you employ, take the time to make two copies or perform the backup twice. This step will provide additional insurance just in case your first backup attempt failed for some reason. If you've ever destroyed a production machine by manipulating the Registry when you didn't have a recent backup, then you'll understand why this hopefully superfluous preparation work is so important. Nine times out of 10, when you don't make the backup, you'll need it.

Restoring the Registry

Obviously, if you intend to take the time to create backups of the Registry, you need to understand how to restore this database. You have several options for restoring the Registry, and maybe more, depending on the method used to make the backup. Windows 2000 itself will attempt to maintain a functional Registry using the fault-tolerance mechanisms already discussed. In cases where the automatic restoration process fails, however, you can first attempt to restore the **Last Known Good Configuration (LKGC)**.

To access this boot option, you press F8 during the initial startup of Windows 2000 when the boot menu is displayed. Don't worry—the basic boot menu even prompts you to press F8 if you need an alternative boot method. Pressing F8 reveals a new selection menu similar to the following:

```
OS Loader v5.0

Windows 2000 Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Restore Mode (Windows 2000 domain
controllers only)
Debugging Mode

Use [up] and [down] to move the highlight to your choice.
Press Enter to choose.
```

Just use the arrow keys to highlight the Last Known Good Configuration selection, then press Enter. The LKGC is the state of the Registry stored in one of the control sets (described earlier in this chapter) when the last successful user logon was performed. If the Registry becomes damaged in such a way that it will not fully boot or will not allow a user

to log on, the LKGC option can restore the system to a previous state. Keep in mind that any changes made to the system between the time the LKGC was stored and when it was used to restore the system will be lost. If the LKGC fails to restore the system to a functioning state, then you have only two options:

1. Use your backup software to restore the Registry files. This operation is possible only if your backup application offers a DOS-based restoration mechanism, which can bypass NTFS write restrictions. In other words, the backup software must operate with a functioning Windows NT environment when launched from a bootable floppy. This type of software lets you restore files to the boot and system partitions (that is, the Registry) so that you can return to a functional operating system. Unfortunately, these applications are rare.
2. Reinstall Windows 2000 either fully or as an upgrade. An upgrade may replace the section of the Registry that is causing the problems, allowing you to retain most of your configuration, but this ability is just the luck of the draw. A full reinstallation of Windows 2000 will return the system to a preconfigured state, requiring you to perform all post-installation changes again.

If you are able to boot into the system but things do not function the way they should or services, drivers, or applications do not load or operate properly, you may need to restore the Registry in part or whole from your backup. Simply use the same tool employed to create the backup to restore the Registry state. Keep in mind that with some tools, you can restore portions of the Registry instead of the entire database at once.

Regardless of which method you choose to restore the Registry, it's always a good idea to restart the system to ensure that the restoration was completed successfully and that the system is using only the updated (or, more correctly, reverted) settings. It is also a good idea to retain the copies of the old Registry until you are confident that the system is functioning normally and you've had an opportunity to create new backups.

Windows 2000 Resource Kit Registry Tools

The **Windows 2000 Resource Kit** includes several utilities which can be brought to bear against the Registry. Because many of these tools are command-line tools or have significant ancillary materials, we recommend that you peruse the Support Tools documentation yourself before actually using them. Some of the key utilities to focus on include the following:

- *Reg.exe:* A tool used to perform command-line operations on the Registry, ideally suited for batch file operations. Functions include querying for value entry data, adding new value entries, changing current values, deleting values or keys, copying keys, backing up and restoring keys, and loading and unloading keys.
- *Regdump.exe:* A command-line tool used to dump all or part of the Registry to the STDOUT file. The output of this tool is suitable for the Regini.exe tool.
- *Regfind.exe:* A command-line tool used to search for a key, value name, or value data based on keywords.

- *Compreg.exe:* A GUI tool used to compare two local or remote Registry keys and highlight all differences between them.
- *Regini.exe:* A command-line scripting tool used to add keys to the Registry.
- *Regback.exe:* A command-line tool used to back up keys from the Registry.
- *Regrest.exe:* A command-line tool used to restore keys to the Registry.
- *Scanreg.exe:* A GUI tool used to search for a key, value name, or value data based on keywords.

TROUBLESHOOTING BOOT FAILURES

Troubleshooting **boot failures** is an essential skill you need to master. It is all too common for errors to occur that will cause a Windows 2000 system to fail to boot. Most of the tasks or actions used to correct problems are fairly simple and logical. In most cases, you'll start with simple solutions and continue to apply more drastic measures until the problem is resolved. The ability to restore a system to boot functionality does not exclude the requirement to maintain a regular and complete backup of your data.

The boot failure troubleshooting process requires four key elements:

- The four Windows 2000 setup boot disks (which can always be built from the CD's \bootdisk directory)
- The Windows 2000 CD and any applied service packs
- An ERD built via the Backup utility
- A recent backup of your Windows 2000 system

The ERD built via the Backup utility under Windows 2000 is not the same as the ERD built via the rdisk /s command under Windows NT 4.0. The Windows NT ERD contains a significant portion of the Registry duplicated by copying files from the systemroot%\repair folder. The Windows 2000 ERD does not contain these Registry files. Instead, its ERD repair process attempts to access the systemroot%\repair folder directly instead of relying on a floppy-based backup. Needless to say, this change on Microsoft's part places less faith in the ERD repair process under Windows 2000 than it did under Windows NT.

With these tools in hand, you can attempt to restore your system to boot functionality by taking the following actions. They are discussed in a general order of simplest to the most complex and drastic.

Advanced Start-up Options

Windows 2000 boasts numerous start-up options not found in Windows NT. These options were borrowed from Windows 95/98 and offer a wider range of capabilities to circumvent boot problems. To access the alternative boot methods, press F8 when the boot menu

appears. You'll see a prompt for this action at the bottom of the screen. Pressing F8 reveals the Advanced Options Menu, which looks like the following:

```
OS Loader v5.0

Windows 2000 Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Restore Mode (Windows 2000 domain
controllers only)
Debugging Mode

Use [up] and [down] to move the highlight to your choice.
Press Enter to choose.
```

From this menu, you can make the following selections:

- *Safe Mode*—Windows 2000 starts using only the minimal drivers and system files. No networking components are loaded.
- *Safe Mode with Networking*—Windows 2000 starts in Safe Mode with network support (this support does not include PC Card networking).
- *Safe Mode with Command Prompt*—Windows 2000 starts in Safe Mode but results in a text-only command prompt instead of the standard GUI desktop.
- *Enable Boot Logging*—This option configures the boot process to write details about loaded drivers and services to the %systemroot%\Ntbtlog.txt file.
- *Enable VGA Mode*—Windows 2000 starts normally but uses only the basic VGA video drivers and resets resolution to 640 × 480 at 256 or 16 colors.
- *Last Known Good Configuration*—Windows 2000 starts using the state of the Registry as stored at the moment of the last successful logon.
- *Directory Service Restore Mode*—Windows 2000 starts and rebuilds/restores the Active Directory. This selection functions on Windows 2000 domain controllers only.
- *Debugging Mode*—Windows 2000 starts and sends debugging information to another system connected by a serial cable. See the *Windows 2000 Resource Kit* for details.

Start-up File Repair

If one of the start-up options does not resolve your boot problems, or if you cannot even reach the boot menu, you may need to replace or repair your start-up files. Although boot

failures are often caused by damaged start-up files, such as Boot.ini, Ntdetect.com, Ntldr, or Ntoskrnl.exe, a damaged **master boot record (MBR)** on the system drive can cause similar problems. The following Repair process can resolve all of these issues:

1. Start the system using the Windows 2000 setup boot disks. After you insert the fourth disk, you'll be prompted for a start-up option. Press the R key to select to Repair a damaged system.
2. Next, you'll be prompted with two additional choices: to repair Windows 2000 using the Recovery Console, or to repair Windows 2000 using the Emergency Repair Process. The Recovery Console option is meant only for advanced users; for details on it, consult the *Windows 2000 Resource Kit* or a Microsoft repair professional. Select the Emergency Repair Process by pressing the R key.
3. Next, you are prompted to decide whether to perform a manual or a fast repair. The manual option offers you the ability to walk through the repair functions one at a time (those functions consist of repair system files, partition and boot sector problems, and start-up and bootstrapping problems). The fast repair performs all of these functions without further prompting. Select either choice.
4. When prompted, provide your ERD or the Windows 2000 distribution CD.
5. Follow any additional prompts that may appear based on the repair process and the problems encountered.
6. Once the repair is complete, the repair process will attempt to restart your computer. Watch for this action, and make sure that all floppies are removed when the reboot occurs.

If your system is not repaired at this point, you have two more options. You can attempt a DOS-based restoration of your backed-up data to restore the system, or you can start over with a fresh installation.

Troubleshooting Printer Problems

Network printers are often the instigators of several affronts to normal productive activity. Printer problems can occur anywhere between the power cable of the printer to the application attempting to print. Systematic elimination of possible points of failure is the only reliable method of resolving printing errors. Here are some common and useful tips for printers:

- Always check the physical aspects of the printer—cable, power, paper, toner, and so on.
- Check the logical printer on both the client and the server.
- Check the print queue for stalled jobs.
- Reinstall the printer driver to make sure it has not become corrupted.
- Attempt to print from a different application or a different client.
- Print using Administrator access.

- Stop and restart the spooler using the Services tool found in Computer Management.
- Check the status and CPU usage of the Spoolss.exe using the Task Manager.
- Check the free space on the drive hosting the spooler file, and change its destination.

This list covers most of the more common print-related problems. For more tips on troubleshooting, consult the *Windows 2000 Resource Kit*.

Troubleshooting RAS Problems

RAS is another area that offers numerous points of failure—from the configuration of the computers on both ends, to the modem settings, to the condition of the communications line. Unfortunately, no ultimate RAS troubleshooting guide exists. Nevertheless, here are some solid steps in the right direction:

- Check all physical connections.
- Check the communications line itself, with a phone if appropriate.
- Verify the RAS installation, the port configurations, and the modem setup.
- Check that both the client and the server dial-up configurations match, including their speed, protocol, and security settings.
- Verify that the user account has RAS privileges.
- Inspect the RAS-related logs: Device.log and Modemlog.txt.
- Remember that multilink and callback will not work together.
- Recognize that autodial and persistent connections may cause the computer to attempt RAS connection upon logon.

Most RAS problems are related to misconfiguration. For more details on RAS, consult the *Windows 2000 Resource Kit*.

Troubleshooting Network Problems

Network problems can range from faults in the media, to misconfigured protocols, to workstation or server errors. Attempt to eliminate the obvious and easy before moving on to more drastic, complex, or unreliable measures. Cabling, connections, and hardware devices are just as suspect as the software components of networking. Verifying hardware functionality involves more than just eyeballing it. You may need to perform some electrical test work, change physical settings, or even update drivers or /ROM BIOS.

Troubleshooting Disk Problems

The component on your computer that experiences the most activity is the hard drive, even when compared to your keyboard and mouse. It should not be surprising that drive failures are common. Windows 2000 is natively equipped to maintain the file system, but even a well-tuned system is subject to hardware glitches. Most partition, boot sector, and drive configuration faults can be corrected or recovered from by using the Disk Management tool. Ultimately, the only truly reliable means of protecting data on storage devices is to maintain accurate and timely backups.

Miscellaneous Troubleshooting Issues

Several troubleshooting tips just don't fit well into the other categories described in this chapter. They are included here in a kind of grab bag of tips.

Permissions Problems

Permission problems typically occur when group memberships conflict or when permissions are managed on a per-account basis. To test for faulty permission settings, attempt to perform the same actions and activities with the Administrator account. Double-check group memberships to verify that no Deny access settings are causing the problem. This step requires examining the ACLs of the objects and the share, if applicable.

It is important to remember that any changes to the access permissions of the individual or groups will not affect those users until the next time they log in. The Access Token used by the security system is rebuilt each time a user logs in.

Master Boot Record

The MBR is the area of a hard drive that contains the data structure that initiates the boot process. If the MBR fails, the ERD cannot be used to repair it. Instead, you'll need to use a DOS 6.0+ bootable floppy and execute "FDISK /MBR". This command will re-create the drive's MBR and restore the system.

Dr. Watson

Windows 2000 includes an application error debugger called **Dr. Watson** that is a diagnostic tool that detects application failures and logs diagnostic details. Data that are captured by Dr. Watson are stored in the Drwtsn32.log file. This feature can also be configured to save a memory dump of the application's address space for further investigation. In reality, the information extracted and stored by Dr. Watson is useful only to a Microsoft technical professional who is well versed in the cryptic logging syntax used.

Windows 2000 automatically launches Dr. Watson when an application error occurs. To configure Dr. Watson, you'll need to launch it from the Start, Run command with "DRWTSN32".

Applying Service Pack Updates

At this point, Microsoft has not released any **service packs** for Windows 2000. But if the company's track record for Windows NT is used as a guide, a service pack will be released soon. A service pack is a collection of code replacements, patches, error corrections, new applications, version improvements, or service-specific configuration settings that correct, replace, or hide the deficiencies of the original product, preceding service packs, or **hot fixes**. A hot fix is similar to a service pack, except that it addresses only a single problem, or a small number of problems, and it may not be fully tested.

Service packs are cumulative, which means that Service Pack 3 (SP3) contains SP2 plus all post-SP2 hot fixes. Thus all you need to install is the latest service pack. You should apply a hot fix only if you are experiencing the problem it was created to resolve; otherwise the hot fix may cause other problems.

A few important points to remember about patches include the following:

- Always back up your system before applying any type of patch, as the backup will give you a way to restore your system if the fix destroys the operating system.
- Be sure to retrieve the correct CPU type and language version.
- Always read the readme and Knowledge Base Q documents for each patch before installing it.
- Update your ERD.
- Make a complete backup of the Registry using the Registry Editor or the REGBACK utility from the Support Tools.
- Export the disk configuration data from Disk Administrator.
- Because service packs rewrite many system-level files, you must disconnect all current users, exit all applications, and temporarily stop all unneeded services before installing any service pack or patch.

To locate Knowledge Base documents, visit or use one of these resources:

- Web site: *http://support.microsoft.com/*
- TechNet CD
- Microsoft Network
- CompuServe: GO MICROSOFT
- Resource Kit Documentation (online help file)

Service packs and hot fixes can be retrieved from the following sources:

- The Web/FTP: *ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/*
- The Web's download section: *http://www.microsoft.com/windows/*

Installing and Uninstalling a Service Pack

To install a service pack:

1. Move the SP file into an empty directory.
2. Close all applications, especially debugging tools.
3. Locate and execute Update.exe with the Start, Run command (see Figure 15-15).

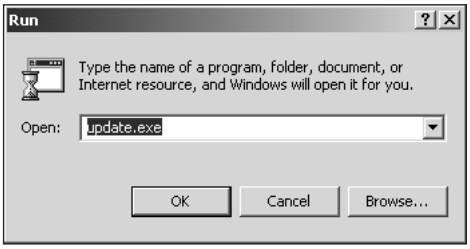

Figure 15-15 Running Update.exe

4. Follow any prompts that appear.
5. When instructed, restart your system.

To uninstall a service pack:

1. You must have selected the "save uninstall information" option during the initial application of the service pack. Whenever it's offered as an option, this choice is usually a good path to take.
2. Extract the original service pack archive into an empty directory.
3. Locate and execute Update.exe.
4. Click the "Uninstall a previously installed service pack" button.
5. Follow the prompts.
6. Restart the computer.

Verifying Service Packs

To determine which service packs have been applied to your system, you can use one of the following techniques:

- Type "WINVER" from a command prompt. This command launches the About Windows information screen, as shown in Figure 15-16.

Figure 15-16 The About Windows information screen

- Select Help, About Windows 2000 from the menu bar of any native tool, such as Windows Explorer.
- Use the Registry Editor to view the CSDVersion value in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion.

Using Microsoft References for Troubleshooting

Several Microsoft resources are available to aid you in troubleshooting and working with Windows 2000:

- Microsoft's Web site—*http://www.microsoft.com/windows/*.
- The Knowledge Base—The predecessor to, and a resource for, the TechNet CD is the online Knowledge Base. It can be accessed by several means, which were detailed earlier in this chapter.
- TechNet—The best periodic publication from Microsoft is TechNet. This multi-CD collection is an invaluable resource containing white papers, FAQs, troubleshooting documents, book excerpts, articles, and other written materials, plus utilities, patches, fixes, upgrades, drivers, and demonstration software. At only $300 for an annual subscription, it is well worth the cost. It is also available online in a limited form at *http://technet.microsoft.com/*.
- Resource Kits—Resource Kits are useful information sources that are available in electronic form through TechNet (in their entirety) and through the online services (in portions). Resource Kits document material outside that contained in Microsoft's manuals, and they often include add-on software utilities to enhance product use.

CHAPTER SUMMARY

- This chapter introduced Windows 2000 troubleshooting techniques, tools, and tips. No matter what problems or errors are discovered on your computer system, there are several common-sense principles of troubleshooting that you should always follow. These principles include performing one task at a time, remaining calm, isolating the problem, and performing the simplest fixes first.
- Information is the most valuable tool needed for troubleshooting. It includes the Computer Information File and a detailed history log of troubleshooting activities.
- Five installation problems are commonly encountered: media errors, domain controller communication difficulties, stop message errors or halt on blue screen, hardware problems, and dependency failures.
- Windows includes several utilities you can use for troubleshooting—most importantly, Event Viewer and the Computer Management tool.
- The Registry is a hierarchical structured database of configuration settings for Windows 2000. It is divided into five keys, each having a unique purpose. When alterations to a system are necessary, it is advisable to use the GUI administration tools first, instead of attempting to edit the Registry directly. Windows 2000 includes two Registry Editors; REGEDIT and REGEDT32. The former is useful for global searches, whereas the latter is useful for changing security settings on keys and value entries. As part of your normal system maintenance and administration, you should create copies of the Registry. Backing up the Registry often is the only way to ensure that you have a functional Registry to restore in the event of a failure.
- Most boot failures can be repaired through the use of a start-up/boot floppy repair process.
- Printer problems are most often associated with physical configuration or spooling problems.
- RAS and network problems are caused by several types of errors, the most common of which is misconfiguration.
- Service packs and hot fixes are used to repair portions of Windows 2000 after the release of the operating system.
- Microsoft has provided several avenues to gain access to information about the operation and management of its products, including a substantial collection of troubleshooting documents.

KEY TERMS

Application log — Records application events, alerts, and system messages.

boot failures — Problems that occur between powering up a computer and the logon prompt display.

Computer Information File (CIF) — A detailed collection of all information related to the hardware and software products that make up your computer (and even your entire network).

Directory Service log — Records events related to the Directory Service.

DNS Service log — Records events related to the DNS Service.

Dr. Watson — The Windows 2000 application error debugger. This diagnostic tool detects application failures and logs diagnostic details.

Event Viewer — The utility used to view the three logs automatically created by Windows 2000.

File Replication Service log — Records events related to the File Replication Service.

HKEY_CLASSES_ROOT — A Registry key that contains the value entries that control the relationships between file extensions (and therefore file format types) and applications. It also supports the data used in object linking and embedding (OLE), COM object data, and file-class association data. This key actually points to another Registry key named HKEY_LOCAL_MACHINE\Software\Classes, and it provides multiple points of access to make itself easily accessible both to the operating system itself and to applications that need access to compatibility information.

HKEY_CURRENT_CONFIG — A Registry key that contains the value entries that control the currently active hardware profile. Its contents are built each time the system is started. This key is derived from data stored in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\HardwareProfiles subkey. It provides backward compatibility with Windows 95/98 applications.

HKEY_CURRENT_USER — A Registry key that contains the value entries that define the user environment for the currently logged-on user. It is built each time a user logs onto the system. The data in this key are derived from the HKEY_USERS key and the Ntuser.dat/.man file of a user's profile.

HKEY_LOCAL_MACHINE — A Registry key that contains the value entries that control the local computer, including its hardware devices, device drivers, and various operating system components. The data stored in this key are not dependent on a logged-on user or the applications or processes currently in use.

HKEY_USERS — A Registry key that contains the value entries that define the user environments for all users who have ever logged into this computer. When a new user logs into the system, a new subkey is added for that user which is either built from the default profile stored in this key or constructed from the roaming user profile associated with the domain user account.

hot fix — Similar to a service pack, except that it addresses only a single problem, or a small number of problems, and may not be fully tested.

key — A top-level division of the Registry. The Windows 2000 Registry contains five keys. Each key can contain subkeys.

Last Known Good Configuration (LKGC) — A configuration recording made by Windows 2000 of all Registry settings that exist at the time when a user successfully logs onto the computer.

master boot record (MBR) — The area of a hard drive that contains the data structure that initiates the boot process.

REG_BINARY — A Registry value entry data type that stores data in binary format.

REG_DWORD — A Registry value entry data type that stores data in binary, hex, or decimal format.

REG_EXPAND_SZ — A Registry value entry data type that stores data in an expandable text-string format that contains a variable that is replaced by an application when it is used (for example, %Systemroot%\file.exe).

REG_MULTI_SZ — A Registry value entry data type that stores data in text-string format that contains multiple human-readable values separated by null characters.

REG_SZ — A Registry value entry data type that stores data in text-string format.

REGEDIT — The 16-bit Registry Editor. REGEDIT offers global searching and combines all of the keys into a single display. It can be used to perform searches, add new subkeys and value entries, alter the data in value entries, and import and export keys and subkeys.

REGEDT32 — The 32-bit Registry Editor. REGEDT32 offers control over key and value entry security but displays each root key in a separate window. It also offers a read-only mode so that you can explore without accidentally altering value entries. REGEDT32 can be used to perform searches, add new subkeys and value entries, alter the data in value entries, and import and export keys and subkeys.

Registry — The hierarchical database of system configuration data that is essential to the health and operation of a Windows 2000 system.

Security log — An Event Viewer log that records security-related events.

service pack — A collection of code replacements, patches, error corrections, new applications, version improvements, or service-specific configuration settings that correct, replace, or hide the deficiencies of the original product, preceding service packs, or hot fixes.

subkey — A sublevel division of a Registry key. A subkey can contain other subkeys and value entries.

System log — An Event Viewer log that records information and alerts about the internal processes of Windows 2000.

value — The actual data stored by a value entry.

value entry — A named Registry variable that stores a specific value or data string. A Registry value entry's name is typically a multiword phrase without spaces that uses title capitalization.

Review Questions

1. When approaching a computer problem, which of the following should you keep in mind? (Choose all that apply.)
   a. How the last problem was solved
   b. What changes were recently made to the system
   c. Information about the configuration state of the system
   d. Your ability to repeat the failure
2. If a media error occurs during installation, which of the following are steps you should take to eliminate the problem? (Choose all that apply.)
   a. Attempt to recopy or reaccess the file that caused the failure.
   b. Switch media sources or types.
   c. Open the Control Panel and reinstall the appropriate drivers.
   d. Restart the installation from the beginning.
3. Which of the following Windows 2000 repair tools can be used to gain information about drivers or services that failed to load?
   a. Event Viewer
   b. Registry
   c. System applet
   d. Dr. Watson
4. The Last Known Good Configuration is useful for which of the following?
   a. Returning the system to the state it was in immediately after the initial installation
   b. Recording a system state for future use
   c. Returning the system to the state it was in at the time of the last successful user logon
   d. Loading a configuration file from floppy disks to use as the current boot parameter file
5. Which Registry Editor should you use if you need to modify the access permissions on a specific key?
   a. REGEDIT
   b. REGEDT32
6. Which of the following are possible troubleshooting techniques for eliminating printer problems? (Choose all that apply.)
   a. Check the physical aspects of the printer—cable, power, paper, toner, and so on.
   b. Check the print queue for stalled jobs.
   c. Attempt to print from a different application or a different client.
   d. Stop and restart the spooler using the Services tool.

7. What is the most common cause of RAS problems?
   a. Telecommunications service failures
   b. Misconfiguration
   c. User error
   d. Communications device failure
8. A user's ability to access a resource is controlled by access permissions. If you suspect a problem with a user's permission settings, what actions can you take? (Choose all that apply.)
   a. Attempt the same actions and activities with the Administrator account.
   b. Delete the user's account and create a new one from scratch.
   c. Double-check group memberships to verify that no Deny access settings are causing the problem.
   d. Grant the user full access to the object directly.
9. Which application automatically loads to handle application failures?
   a. Event Viewer
   b. System applet
   c. Computer Management
   d. Dr. Watson
10. After installing a new SCSI driver, Windows 2000 will not start. No other changes have been made to the system. What is the easiest way to return the system to a state where it will start properly?
    a. Use the repair process with the ERD.
    b. Use the Last Known Good Configuration.
    c. Configure Dr. Watson.
    d. Boot to DOS, and run the setup utility to change the installed drivers.
11. Which of the following are important actions to perform before installing a service pack or a hot fix? (Choose all that apply.)
    a. Make a backup of your system.
    b. Read the readme and Knowledge Base Q documents.
    c. Make a complete backup of the Registry.
12. The Registry is the primary data storage mechanism for Windows 2000. Which of the following are data storage files used by other Microsoft operating systems that may still exist on Windows 2000 for backward compatibility purposes? (Choose all that apply.)
    a. Win.ini
    b. Autoexec.bat
    c. System.ini
    d. Config.sys

13. The Registry is used only to store configuration data for native Windows 2000 applications, services, and drivers. True or False?
14. Which of the following tools are most highly recommended by Microsoft for editing the Registry? (Choose all that apply.)
    a. Control Panel applets
    b. REGEDIT
    c. Reg.exe
    d. Administrative Tools
15. The Registry is an exhaustive collection of system control parameters. True or False?
16. When editing the Registry, and especially when attempting to alter the unseen defaults, which of the following pieces of information are important? (Choose all that apply.)
    a. Syntax
    b. Spelling
    c. Subkey location
    d. Valid values
    e. Time zone
17. Changes made to the Registry never go into effect until the system restarts. True or False?
18. Which of the following can host subkeys or value entries?
    a. Data type
    b. Key
    c. Subkey
    d. Value data
19. Each of the five keys of the Registry is stored in a distinct file on the hard drive. True or False?
20. Which Registry key contains the value entries that control the local computer?
    a. HKEY_LOCAL_MACHINE
    b. HKEY_CLASSES_ROOT
    c. HKEY_CURRENT_CONFIG
    d. HKEY_USERS
21. Which Registry key contains the value entries that define the user environment for the currently logged-on user?
    a. HKEY_LOCAL_MACHINE
    b. HKEY_CLASSES_ROOT
    c. HKEY_CURRENT_CONFIG
    d. HKEY_CURRENT_USER

22. Which Registry key contains the value entries that control the relationships between file extensions (and therefore file format types) and applications?
    a. HKEY_LOCAL_MACHINE
    b. HKEY_CLASSES_ROOT
    c. HKEY_CURRENT_CONFIG
    d. HKEY_USERS
23. Which Registry key contains the value entries that control the currently active hardware profile?
    a. HKEY_LOCAL_MACHINE
    b. HKEY_CLASSES_ROOT
    c. HKEY_CURRENT_CONFIG
    d. HKEY_CURRENT_USER
24. From which key can you delete subkeys using the System applet?
    a. HKEY_LOCAL_MACHINE
    b. HKEY_CLASSES_ROOT
    c. HKEY_CURRENT_CONFIG
    d. HKEY_USERS
25. The files used to load the Registry at startup are stored where on a Windows 2000 system?
    a. %systemroot%\config
    b. %systemroot%\system32\config
    c. %systemroot%\system\config
    d. %systemroot%\system32\repair

HANDS-ON PROJECTS

Project 15-1

To use the Event Viewer:

1. Open the **Event Viewer** from the Start menu (Start, Programs, Administrative Tools, Event Viewer).
2. Select the **System log** from the list of available logs in the left pane (refer back to Figure 15-1).
3. Notice the various types of events that appear in the right pane.
4. Select an event in the right pane.
5. Select the **Properties** command from the **Action** menu.
6. Review the information presented by the event detail (refer back to Figure 15-2).

7. Click the up and down arrows to view other event details.
8. Click **OK** to close the event detail.
9. Close the Event Viewer by clicking the **X** button in the upper-right corner of the title bar.

Project 15-2

To view the Registry through REGEDIT:

1. Open the Run command by selecting **Start**, **Run**.
2. Type **regedit**, then click **OK**. The Registry Editor opens (refer back to Figure 15-4).
3. Double-click **HKEY_LOCAL_MACHINE** (refer back to Figure 15-5).
4. Locate and double-click **SOFTWARE** under HKEY_LOCAL_MACHINE.
5. Locate and double-click **Microsoft** under SOFTWARE.
6. Locate and double-click **Windows NT** under Microsoft.
7. Locate and double-click **CurrentVersion** under Microsoft.
8. Locate and select **Winlogon** under CurrentVersion.
9. In the right pane, locate and select **DefaultUserName** (see Figure 15-17).

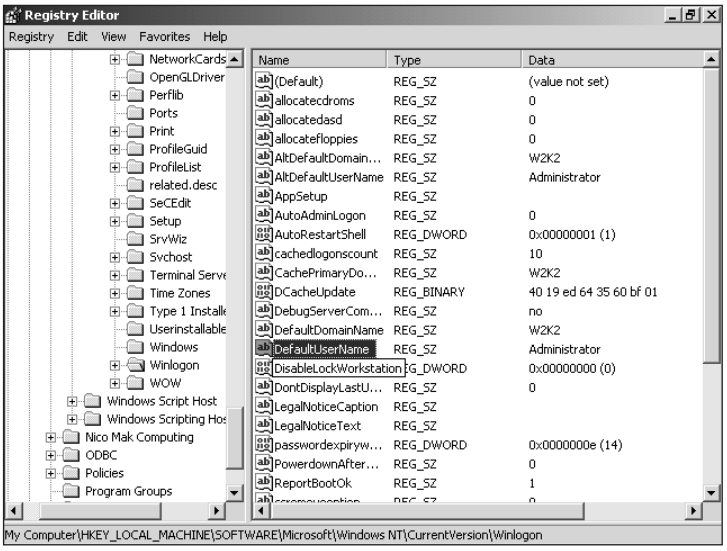

Figure 15-17 The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin key, DefaultUserName value

10. Select **Modify** from the **Edit** menu.
11. Notice that the value of this value entry is the name of the user account you are currently using (see Figure 15-18).

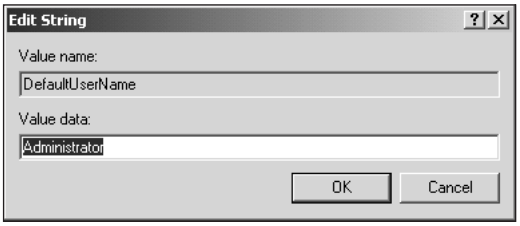

Figure 15-18 The Edit String window

12. Click **Cancel**.
13. In the left pane, scroll up until you see HKEY_LOCAL_MACHINE.
14. Double-click **HKEY_LOCAL_MACHINE**.

Project 15-3

To search for a value entry with REGEDIT:

This Hands-on Project requires that Hands-on Project 15-2 be completed.

1. Select **Find** from the **Edit** menu.
2. In the **Find what** field, type **DefaultUserName** (see Figure 15-19).

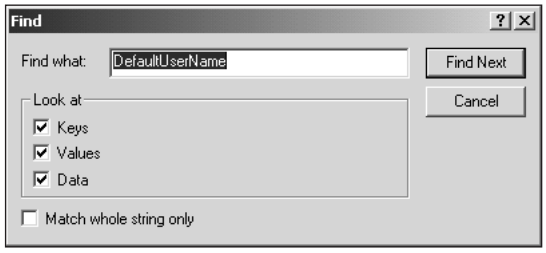

Figure 15-19 The Find window in Registry Editor

3. Click **Find Next**.
4. After a few seconds of searching, REGEDIT will locate the first key, value, or data containing that string. Notice that the first found match is AltDefaultUserName.
5. Select **Find Next** from the **Edit** menu.
6. Notice that item found now is the actual DefaultUserName value entry that you viewed in Hands-on Project 15-2.
7. In the left pane, scroll up and double-click **HKEY_LOCAL_MACHINE**.

Project 15-4

To save a Registry key:

1. Make sure that the **HKEY_USERS** key is selected.
2. Select **Export Registry File** from the **Registry** menu.
3. Select a destination folder of your choice.
4. Provide a filename, such as **HUsave.reg** (see Figure 15-20).

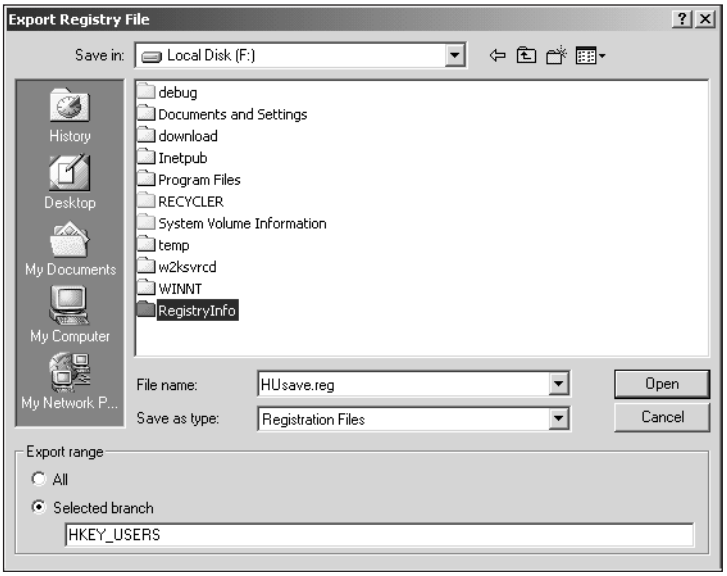

Figure 15-20 Exporting a Registry file

5. Make sure that the **Selected branch** radio button at the bottom of the Export Registry File dialog box is selected and that **HKEY_USERS** is listed in the text field, as shown in Figure 15-20.
6. Click **Save**. REGEDIT will create a backup file of the selected key.

Project 15-5

To restore a Registry key:

Note: This Hands-on Project requires that Hands-on Project 15-4 be completed.

Note: If you have made any change to the system or Registry since you completed Hands-on Project 15-3, you may not want to do this project as it will discard those changes by restoring the state of the Registry from the saved file.

1. Select **Import Registry File** from the **Registry** menu.
2. Locate and select your **HUsave.reg** file.
3. Click **Open**.

4. After a few moments of importing, a message stating whether the import succeeded is displayed. Click **OK**.
5. Select **Exit** from the **Registry** menu.

Project 15-6

To use REGEDT32:

1. Open the Run command by selecting **Start**, **Run**.
2. Type **regedt32**, then click **OK**. The Registry Editor opens.
3. Notice that each key is displayed in a separate window within the Registry editor.
4. Select **HKEY_LOCAL_MACHINE** from the **Window** menu.
5. Select **Find Key** from the **View** menu.
6. Type **DefaultUserName**.
7. Click **Find Next**.
8. Notice that you are back in the same subkey as was viewed in Hands-on Project 15-1.
9. Select **Read Only Mode** from the **Options** menu.

Project 15-7

To view security with REGEDT32:

Note: This Hands-on Project requires that Hands-on Project 15-6 be completed.

1. Select **HKEY_USERS** from the **Window** menu.
2. Select **Permissions** from the **Security** menu.
3. A notice may appear indicating that you can only view permissions for this key. Click **OK**.
4. Notice that the Permissions dialog box for the Registry is identical to that used elsewhere in Windows 2000.
5. Click **Cancel**.
6. Select **Exit** from the **Registry** menu.

CASE PROJECTS

1. After you installed a new drive controller and a video card, along with their associated drivers, Windows 2000 refuses to start and the LKGC does not result in an operational system.

   Required Result:

   Return the system to a bootable and operational state.

Optional Desired Results:

Retain the security ID.

Retain most, if not all, of the system's configuration.

Proposed Solution:

Perform a complete reinstallation of Windows 2000.

a. The proposed solution produces the desired result and both of the optional desired results.
b. The proposed solution produces the desired result, but only one of the optional desired results.
c. The proposed solution produces the desired result, but neither of the optional desired results.
d. The proposed solution does not produce the desired result.

2. After you install a new drive controller and a video card, along with their associated drivers, Windows 2000 refuses to start and the LKGC does not result in an operational system.

   Required Result:

   Return the system to a bootable and operational state.

   Optional Desired Results:

   Retain the security ID.

   Retain most, if not all, of the system's configuration.

   Proposed Solution:

   Perform an upgrade reinstallation of Windows 2000.

   a. The proposed solution produces the desired result and both of the optional desired results.
   b. The proposed solution produces the desired result, but only one of the optional desired results.
   c. The proposed solution produces the desired result, but neither of the optional desired results.
   d. The proposed solution does not produce the desired result.

3. You need to perform several Registry modifications to fine-tune an application. You'll be following detailed instructions from the vendor. What steps can you take to ensure that even if the vendor's instructions fail, you'll still be able to return to a functioning Windows 2000 system?

4. Describe the common problems associated with installing Windows 2000 and the steps you can take to either avoid these problems or resolve them once encountered.